PATENT ABSTRACTS OF JAPAN

(11)Publication number:

11-239125

(43) Date of publication of application: 31.08.1999

(51)Int.CI.

H04L 9/08

(21)Application number: 10-040641

(71)Applicant: NIPPON TELEGR & TELEPH CORP

(22)Date of filing:

23.02.1998

(72)Inventor: KAWABATA MICHIO NIHEI KATSUTOSHI

NAKAYAMA MASAYOSHI

ARAKI KATSUHIKO

(54) METHOD AND SYSTEM FOR CRYPTOGRAPHIC COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To remarkably increase the number of session keys and master keys handleable at an information transmission station by reducing the number of pieces of key information for change by transmitting the session key, which is enciphered by each master key for destination, just for plural destinations.

SOLUTION: When changing the session key, first of all, the destination is turned into destination to change the session key by a key managing server 11 at the information transmission station, a newly generated session key is enciphered by the master key for session key distribution for each destination, and key information for change is generated and transmitted. Afterwards, key application timing information is generated for reporting the application timing of the new session key transmitted by the key information for change to an information reception station and the destination is transmitted as the destination to change the session

key. Besides, together with the transmission of key change timing information, the session key for the relevant destination preserved in a session key retrieving part 13 is changed to the new session key.

(19) 日本国格群庁 (JP)

€ 獓 ধ 盂 华 噩 **₹**

梅開平11-239125

(11) 格許田國公園梅中

(43)公開日 平成11年(1999) 8 月31日

601B 601A 601E 8 H04L H04L 9/08 (51) Int.C.

(全13月) 審査請求 未請求 請求項の数10 01.

(21)出现番号	特取平10-40841	(71) 出版人 000004226	000004226
			日本電信電腦株式会社
(22) 出間日	平成10年(1998) 2 月23日		東京都新信区西新宿三丁目19年2号
		(72) 発明者	を を を を を を を を を を を を を を を を を を を
			東京都新宿区西新宿三丁目19番2号 日本
			自信电影探式会社内
		(72) 発明者	作 中 日本
			東京都新宿区西斯宿三丁目19番2号 日本
			每位复招株式会社内
•		(72)発明者	中山 正芳
			東京都新信区西新信三丁目19番2号 日本
			真質質語株式会社内
		(74) 代理人	(74)代理人 弁理士 三好 秀和 (外1名)
			最終同に扱く

(54) 【発明の名称】 昨号化通信方法および暗号化通信システム

昨号化を可能にすると共に、変更用壁情報等の送信数を 【歌題】 本発明は、番組単位のみならず受信局単位の 極力、小さくすることのできる暗号化通信方法および暗 **身化通信システムを提供することを目的とする。**

を保持し、前記伝送情報を受信したときには当該受信娼 **号化し、加配セッション鍵を変更する際には前記変更用** 【解決手段】 情報送信局は、全宛先用のセッション鍵 およびマスタ戯とを保持し、伝送情報を送信するときに は当該伝送情報の充先に対応するセッション鍵を用いて 伝送情報を暗号化して送信し、前配セッション鍵を変更 する際には変更用壁筒報に複数の充先に対応するセッシ ョン駐をマスタ壁で暗号化して送信し、受信焰末は、割 り当てられる宛先用のセッション鍵と宛先用マスタ盤と 末に記憶されるセッション顔を用いて当該伝送情報を復 **単情報を受信して前記記憶手段に記憶されるマスタ壁を** 用いて復号して変更されたセッション健を得る。

6-t/I £Ŗ

** 3000 THE RESERVE AS A STATE OF

8

校団早11-239125

ョン観を変更する際に前記変更用題物数を受信して前記 送情報を復号化する伝送情報復号化手段と、前配セッシ 記憶手段に記憶されるマスタ壁を用いて復号して変更さ れたセッション観を得る変更用観情報復号化手段と有す ることを特徴とする時号化通信システム。 与された伝送情報を送信し、この伝送情報を当該宛先の 受信端末で受信し復号化するときの暗号化通信方法であ

「請求項1】 情報送信局で暗号化され所定の宛先が付

特許額水の範囲

[開水収7] 前配変更用壁情報は、各紀先用の壁変更 報に従って前配情報送信局および当該宛先の各情報受信 タイミング情報と共に送信され、当駐坂里タイミング信 応にカッツョン部や低しいカッツョン部に仮以するいか を特徴とする請求項6配做の暗号化過信システム。 01

情報送信局は、全宛先用のセッション健およびマスタ健 とを配慮し、伝送情報を送信するときには当該伝送情報

の宛先に対応するセッション雌を用いて伝送情報を暗号

ö

【韓水瓜8】 的記憶像送信局は、変更用館情像及び館 変更タイミング情報を複数回線り返して送信することを [請求項9] 前記情報送信局は複数であることを特徴 特徴とする静水項6または7配娘の時号化通信システ

記憶し、前記伝送情報を受信したときには当該受信端末

に記憶されるセッション鍵を用いて当該伝送情報を復号 前記セッション健を変更する際には、情報送信局は、こ の情報送信局より送信される変更用難情報に複数の宛先

受信臨末は、当該受信臨末が受信資格のあるときに関り

当てられる宛先用のセッション健と宛先用マスタ姫とを

【韓状版10】 在記セッション邸の仮更は、校更周期 が各角先毎に変えて行われることを特徴とする請求項の とする語状氏 6、7または8記録の最中化過信システ 乃至9のいずれかに配做の時母化通信システム。

[発明の詳細な説明] [000]

2

受信端末は、前記変更用燈情報を受信したときには前記 受信端末に記憶されるマスタ鍵を用いて復号し、変更さ

に対応するセッション騒をマスタ戯で暗号化して送信

れたセッション観を得ることを特徴とする時号化通信方 [請求項2] 前記変更用館情報は、各宛先用の鏈変更 タイミング情報と共に送信され、当顧変更タイミング情 報に従って前配情報送信局および当政宛先の各情報受信 局はセッション館を新しいセッション館に変更すること

[発明の属する技術分野] 本発明は、情報送信局から受 間臨来への通信を提供する通信システムにおける時身化

[従来の技術] 近年、韓国放送が普及してきており、こ の衛品放送では有料放送の映像や音声等に対してスクラ ンンノを値ずことにより不正的場を防ぐようにしてる。 通信方法および暗号化通信システムに関するものであ 39

> [静水項3] 前記情報送信局は、変更用壁情報及び壁 変更タイミング情報を複数回線り返して送信することを 【静水項4】 前配荷報送信局は複数であることを特徴

を特徴とする翻水項1配線の暗号化通信方法。

持徴とする請求項1または2配娘の時号化通信方法。 とする群状項1、2または3記載の暗号化通信方法。

このような慎重放送で用いられているスクランブル方法

[0003]図15において、 概Ksは協能室の設能感 **/デスクランブル処理を行うための館で、鴟Kwは番組** と受信息のBS デューダで正しく対応したスクランブル 資金の指令の概で、低KmはBS(Brondenst ing sotellite;放送徴回) ゲコーダ年に の3.血管暗母の概要を図1.5に示す。

【朝水瓜 2】 「前記セッション艇の変更は、変更周期が

各宛先毎に変えて行われることを特徴とする請求項1乃 【請求項6】 情報送信局で暗号化され所定の宛先が付 与された伝送情報を送信し、この伝送情報を当該宛先の

至4のいずれかに記載の暗号化通信方法。

ランダムゲータ列を発生するために、スクランブルの値 ・由声信母をデスクランプルすることになる。この模似 **大きが沿られるが、意大きは存在在的の一部ソフト語学 行されており、BSゲコーダではいれを称く壁Kwがな 問として語号化されており、BSゲコーダ因在の題Km** がないと暗号解脱できない。さらに、この睫Kwを含ん が個別情報は、視聴料金を納めた視聴者だけに遺信され る。 健KmはBSゲコーダ毎に異なるため、祝愿特会来 **樹者のBSゲコーダでは暗母の復身ができず、億Kwを** [0004] この図15に示す方法では、BSデコーダ では送信局と同じ疑囚タンダムゲータ列を発生し、映像 いと暗号解節できない。さらに、健Kwは個別情報の― 因有の個別情報の暗身の駐である。

9

情報送信局は、全宛先用のセッション戯およびマスタ戯

受信端末で受信し復号化するときの略号化通信システム

とを配慮する配億手段と、伝送物報を送信するときには 当故伝送情報の充先に対応するセッション戯を用いて伝 送情報を暗号化して送信する伝送情報暗号化手段と、前 配セッション雌を変更する際に変更用雌惰報に複数の宛 先に対応するセッション鍵をマスタ鍵で暗号化して送信 受信端末は、当該受信端末が受信資格のあるときに割り 当てられる宛先用のセッション艇と宛先用マスタ艇とを

-5

S

記憶する記憶手段と、前記伝送情報を受信したときには 当該受信端末に記憶されるセッション観を用いて当該伝

する変叉用鏈情報暗号化手段とを有し、

のデスクランブルに必要な情報を担って約1秒に1回送 信される。このため、BSデコーダが番組情報を取り落 [0005] この方法において、番組債額は壁Ksなど とすと、この直後約1秒は臨実にデスクランブルできな くなってしまう。そこで同じ番組債報を複数回連競送信 して受信仰で多数決判定できるようにしている。

アルゴリズムは、映像信号のライン毎に切れ目を入れ左 右を入れ替えるラインローテーションや、映像信号のラ インを入れ替えるラインパーミュテーションなどが用い 【0006】また、この方法で用いられるスクランブル

採用している。このため、暗号化はMPEG2のトラン スポートストリームという情報単位で行い、暗号化アル [0007] また、CS (Communication 上記の方法と同僚に、鮭構成は3層で、暗号化はDVB ng) との共通化を図るため、MPEG2 Video &AudioおよびSystemsを介格とした方式を ゴリズムは共通健時号法の1つであるMulti2の壁 及32ビット以上の値を用いて行っている。この方法で は、最大96種類のトランスポートストリームに対し異 (Digital Video Broadcasti satellite;通信衛星) デジタル放送では、 なる蛆を用いて暗号化を行うことができる。

ittee, Phase IATM Security Transfer Mode;非同期転送モード)を 用いた片方向通信システムでのセッション壁の変更法が ATM Forum Technical Comm Specification (Draft), Sep tember, 1997」に示されている。このセッシ ョン健変更法を以下に示す。

[0008] また、ATM (Asynchronous

【0009】まず、セキュリティ向上のために行うセッ ション壁の変更は、各番粗用のマスタ壁を各番組の受信 資格を持つ全ての受信局に干め与えておく。

AM (Operation, Administrati のマスタ鍵で暗号化しセッション鍵送信用のSKE O 【0010】情報送信局でセッション観を変更する番組 用の新しい鍵を生成し、生成した新しい鍵を当該番組用 on and Maintenance;運用保守) セ ルに組み込み送信する。この番組の受信資格を持つ各受 **予め与えられたこの番組用マスタ鍵で、受信した番組用** SKE OAMセルを復母化し、矩しいセッション戯を 信局では、当政番組用のSKE OAMセルを受信後、

【0011】その後、情報送信局は、番組用の離変更タ に、当該情報送信局における当該番組用のセッション壁 イミング通知用のSKC OAMセルを送信すると共

ョン戯に変更する。また、この番組の受信資格のある金 ての受信局で当該番租用のSKC OAMセルを受信す ると同時に当該番組用セッション鍵を新しいセッション 酸に変更する。

送来の片方向通信用暗号化方式は、BS放送用、CS放 送用等、複数の受信局で同じ情報を受信する番組毎に異 |発明が解決しようとする課題| 上述してきたように、 なるセッション競及びマスタ鍵を持つ暗号化方式であ 【0013】しかしながら、最近では衛盘通信等の片方 向通信を用いて1受信局に対してのみ情報を送信したい という舒要がある。また、ATM Forumに示され ているSKE OAMセル及びSKC OAMセルを用 いるセッション壁の変更法を、受信局毎に異なるセッシ OAMセル及びSKC OAMセルは各受信局毎に異な るセルを送信する必要があるため、SKE OAMセル 及びSKC OAMセルの送信数は受信局の増加に伴い 大きくなり、通信システムの通信帯域に大きな影響を与 える。このため、変更用盤情報及び盤変更タイミング情 ョン鍵を用いるシステムに適用する場合には、SKE 頼の送信数をできるだけ小さくしたいという課題があ

周単位の暗号化を可能にすると共に、変更用鍵情報及び のできる暗号化通信方法および暗号化通信システムを提 [0014] 本発明は、上記課題に鑑みてなされたもの で、情報送信局で扱えるセッション鍵、マスタ鍵の数を 飛躍的に大きくすることにより番組単位のみならず受信 **豊変更タイミング情報の送信数を極力、小さくすること** 供することを目的とする。

[0015]

ために、本発明のうちで請求項1記載の発明は、情報送 信し、この伝送情報を当該宛先の受信端末で受信し復号 全宛先用のセッション健およびマスタ健とを記憶し、伝 当てられる充先用のセッション雌と宛先用マスタ雌とを 配飾し、前配伝送情報を受信したときには当該受信端末 に記憶されるセッション鍵を用いて当該伝送情報を復号 化し、前記セッション鍵を変更する際には、情報送信局 の宛先に対応するセッション鍵をマスタ鍵で暗号化して 【0016】このとき、変更用戯情報はセッション壁を 【蝶題を解決するための手段】前述した目的を達成する 信局で暗号化され所定の宛先が付与された伝送情報を送 送情報を送信するときには当該伝送情報の宛先に対応す 受信端末は、当該受信端末が受信資格のあるときに割り は、この情報送信局より送信される変更用触情報に複数 送信し、受信臨末は、前記変更用館情報を受信したとき には前記受信端末に記憶されるマスタ鍵を用いて復号 るセッション鍵を用いて伝送情報を暗号化して送信し、 し、変更されたセッション戯を得ることを要旨とする。 化するときの暗号化通信方法であって、情報送信局は、

9

b良い。さらには各宛先年に当該宛先用のマスタ壁で暗 **身化した複数のセッション鍵を変更用壁情報に配破する** もであっても良く、また複数のセッション鍵をマスタ母 マスタ鍵で暗号化したものを配斂するものであっても良 く、あるいは新規に生成した各宛先用のセッション鍵を マスタ鍵で暗号化して変叉用壁情報としたものであって で暗号化したものであっても良い。

更用値情報を、複数の宛先で同時に受信できる変更用値 情報配送用の宛先を準備し、各宛先用のマスタ壁で暗号 セッション鮭の変更の際に、情報送信局より送信する変 化したセッション艇を複数の宛先分送信して変叉用戯情 [0017] これにより、請求項1記載の本部用では、 報の数を削減する。

記載の変更用鮭情報は、各宛先用の健変更タイミング情 限と共に送信され、当燈変更タイミング情報に従って前 配付報送信局および当該宛先の各情報受信局はセッショ [0018] また請求項2記載の発用は、前記請求項1 ン鍵を折しいセッション鍵に変更することを要旨とす

セッション醚の変更の際に、情報送信局より各宛先用の 変更用雌情報を送信し、各変更用雌情報で送信した雌の 育姫により行い、送信する韓変更タイミング情報の数を 適用は全宛先において1つの宛先用の壁変更タイミング [0019] これにより、請求項2記載の本発明では、

または2記載の情報送信局は、変更用駐情報及び健変更 タイミング情報を複数回線り返して送信することを要旨 [0020]また請求項3記載の発明は、前記請求項1

各情報受信局においてセッション鮭の変更を失敗する確 [0021]これにより、請求項3配破の本発明では、 事が小さくなる。

2

1、2または3記載の情報送信局は複数であることを要 [0022] また請求項4記載の発明は、前記請求項 旨とする。

乃至4のいずれかに配做のセッション観の変更は、変更 必要に応じてセッション娘の変更周期を、安全性と、変 **更用飽情報及び餓変更タイミング情報の送信によるシス** アムの送信符換への影響とのトレードオンにより決定す [0024] また請水項5記載の発明は、前記請水項1 【0023】これにより、額水項4配穀の本発明では、 [0025] これにより、簡本項5配銀の本発明では、 **周期が各知先毎に変えて行われることを要旨とする。** 1 つの情報送信局にかかる処理负荷が軽減される。

この伝送情報を当該宛先の受信端末で受信し復号化する ときの暗号化通信システムであって、情報送信局は、全 宛先用のセッション鍵およびマスタ壁とを記憶する記憶 [0026] また請求項6記載の発明は、情報送信局で 暗号化され所定の宛先が付与された伝送情報を送信し、

冬至中11-239125

€

経情報を受信して前記記憶年段に記憶されるマスタ壁を 用いて位与して変更されたセッション騒を得る変更用態 **再段と、伝送情報を送信するときには当該伝送情報の宛 ト送信する伝送信報時号化手段と、前記セッション館を** 変更する際に変更用駐情報に複数の宛先に対応するセッ ション騒をマスタ壁で暗号化して送信する変叉用壁情報 昨号化平段とを有し、受信臨末は、当該受信臨末が受信 資格のあるときに割り当てられる気先用のセッション酸 報を受信したときには当該受信臨末に記憶されるセッシ ョン鍵を用いて当該伝送情報を復与化する伝送情報復与 化手段と、前記セッション観を変更する際に前記変更用 先に対応するセッション粗を用いて伝送情報を暗号化し と宛先用マスタ銀とを配値する配億手段と、前配伝送情 情報復母化手段と有することを受管とする。 2

Å

更用動情報を、複数の角先で同時に受信できる変更用師 慣報配送用の宛先を準備し、各宛先用のマスタ雄で暗号 セッション娘の変更の際に、情報送信局より送信する数 化したセッション艇を拉数の宛先分送信して蛟叉用艇情 [0027] これにより、請求項6記録の本発明では、 缶の数を削減する。

私と共に送信され、当燈敷贝タイミング情俗に従って信 配情報送信周および当該充先の各情報受信回はセッショ [0028] また請求項7記録の発明は、前記請求項6 配位の変更用値情報は、各紀先用の態変更タイミング情 ン鍵を折しいセッション鍵に変更することを受管とす

セッション館の変更の際に、情報送信局より各組先用の 変更用磁情報を送信し、各変更用磁情報で送信した壁の 適用は全気先において 1 つの気先用の触変更タイミング 情報により行い、送信する難変更タイミング情報の数を [0029]にれにより、簡水瓜7配板の本発明では、

[0030] 虫た鯖水瓜8配做の殆兜は、向記閣氷瓜8 または7記載の情報送信局は、変更用館情報及び健変更 タイミング情報を複数回線り返して送信することを要拒

各情報受信局においてセッション艇の変更を失敗する頃 [0031] これにより、請求囚8的債の本発明では、

6、7または8配線のሰ船送信局は複数であることを要 [0032] また間水瓜の配板の発明は、前配静水斑 事が小さくなる。 \$

[0034] また前水項10記載の発明は、前記請水町 8 乃至9 のいずれかに記載のセッション館の疫更は、疫 [0033]これにより、請求項9配板の本発明では、 **更周期が各和先毎に変えて行われることを更旨とする。** [00:35] これにより、請水瓜10紀億の本発用で 1 しの哲館设備原にかかる処理女母が酷談される。

と、変更用館情報及び随変更タイミング情報の遺信によ

ಜ

は、必要に応じてセッション鮭の変更周期を、安全性

20

を、SKC OAMセルの送信と回時に、新しいセッツ

[0036] すなわち、本発明における暗号化通信方法 段より高辺に彼霜し、彼霖されたセッション騒を用いて 前記入力情報を暗号化する暗号手段と、セッション鍵の **堕で暗号化した情報を記載した変更用壁情報を作成、送** のセッション鍵を新しいセッション健に変更する手段を およびこの方法が適用されるシステムでは、情報送信局 は、全宛先用のセッション鍵を宛先順に配像する配像手 入力价铅を配億する配億年段を持ち、情報送信局に送信 た宛先用のセッション雄を、前記セッション艇の配像手 変更の際に、各充先で用いる新しいセッション離を生成 当宛先用のマスタ鍵を前記マスタ鍵の記憶手段より **信する手段と、変更用盤情報送信後にセッション壁の変 更を行った宛先と新しいセッション壁の情報より、当瞭** 宛先用の壁変更タイミング情報を作成、送信すると同時 備え、受信端末は、受信資格のある宛先用のセッション **睦、受信資格のある宛先用のマスタ壁及び受信情報を記** 億する記憶手段を持ち、受信端末に入力された受信情報 **端末内のセッション燈の記憶度域より検索し、検索した** と、受信した変更用壁物報の宛先を参照し、参照した宛 先用のマスタ鍵を受信端末内のマスタ艇の配値領域より 検索し、検索したマスタ戯を用いて変更用壁情報を復号 化する復号手段と、壁変更タイミング情報受信時に、受 信した餓疫更タイミング情報の宛先用の新しいセッショ 情報が入力されると、入力情報の宛先を参照し、参照し 高速に検索し、新しいセッション鍵を検索されたマスタ に情報送信局内のセッション壁の記憶手段の当政宛先用 の宛先を参照し、参照した宛先用のセッション鍵を受信 ン壁を受信端末内にある当該宛先用のセッション鍵記憶 全宛先用のマスタ鍵を宛先順に記憶する記憶手段、 セッション鍵を用いて受信情報を復与化する復号手段

- タベースに蓄積、保存される。

情報送信局より送信する各変更用鍵情報を、複数の宛先 し、各宛先用のマスタ壁で暗号化したセッション壁を複 数の宛先分配做、送信することにより送信する変更用鍵 [0031] これにより、セッション韓の叛更の際に、 で同時に受信できる変更用健情報配送用の宛先を準備 情報の数を削減することが可能となる。

領域に審き込む手段とを具備する。

[0038]また、セッション鮭の変更の際に、情報送 信局より各紀先用の変更用館情報を送信し、各変更用館 情報で送信した壁の適用は全宛先において1 つの全宛先 用の母変更タイミング情報により行うことにより、送信 する雄変更タイミング情報の数を削減することが可能と

【発明の契縮の形態】以下、図面を用いて本発明の実施 **の形態にしてた気配する。**

8 通信方法が適用される暗号化通信システムの情報送信局 [0040]図1は本発明の一実施の形態に係る暗号化

受信局の要問の構成を示すプロック図である。図1に示 の要部の構成を示すプロック図であり、図2は同、情報 **す情報送信局は聲管理サーベ1.1、セッション聲換索部** 育報受信局はセッション健抽出部22、セッション健検 | 3およびエンコーダ15により構成され、図2に示す **報節25およびデコーダ26により構成される。**

【0041】図1に示す情報送信局内のセッション壁検 **森郎13では全ての充先用のセッション壁を保存してお** 資格を持つ宛先用の全てのマスタ鍵を保存しているもの を保存し、セッション聲抽出師22では当受信局で受信 とする。なお、これらセッション雌とマスタ鍵は図示し ン鍵配信用のマスタ鍵を保存しているとする。また、図 2 に示す情報受信局のセッション鍵検索部25では、情 報受信局で受信資格を持つ宛先用の全てのセッション離 ないハードディスク、光学的配値媒体等で構成されるデ り、健管理サーベ11内には、全ての危先用のセッショ

[0042] 図1において情報受信局では、パケット形 構成される。まず、送信される伝送情報(以下、単に送 情情報)がエンコーダ15に入力されると、エンコーダ 15ではパケットの充先情報を抽出しセッション鍵検索 ったセッション鍵を用いて受信したパケットの宛先情報 式の情報は宛先情報と実際に送信される伝送情報とから エンコーダ13に送出する。エンコーダ13では受け取 耶13に送信し、当該宛先用のセッション鍵を検索し、 と除いた送信符報のみを暗号化し、送信する。

2

【0043】情報受信局においては図2に示すように情 **現送信局から送信され情報受信局で受信された伝送情報** (以下、単に受信情報) がデコーダ26に入力されると 受信情報の宛先情報をセッション壁検索部25に送信

し、当該允先用セッション鍵を検索し、デコーダ26に 用いて、受信パケットの充先情報を除いた受信情報のみ 送信する。デコーダ26では受け取ったセッション離を を復号化し、出力する。

報を生成し、宛先をセッション鍵変更を行う宛先とし送 育報送信局の駐管理サーバ11で、まず宛先を、セッシ / 健を各宛先用のセッション観配送用のマスタ鍵で暗号 化して変更用雌情報を生成し、送信する。その後、変更 **がを情報受信局に知らせるための、健適用タイミング情 間する。また、壁変更タイミング情報の送信とともにせ** ッション壁検索部13に保存している当宛先用のセッシ [0044] セッション鮭の変更の際には、図1に示す ョン雌の変更を行う宛先とし、新しく生成したセッショ 用壁情報で送信した新しいセッション鮭の適用タイミン ョン鍵を新しいセッション鍵に変更する。

\$

すると、セッション健抽出部22で、予め保存している 当宛先用のマスタ戯で変更用録情報を復号化し新しいセ [0045] 一方、図2に示す情報受信局では、当版情 **租受信局で受信資格のある和先用の変更用鏈情報を受信** ッション鍵を得る。その後、当宛先用の鍵変更タイミン

7情報を受信すると同時にセッション競技索部25に保 存している当宛先用のセッション壁を新しいセッション

9

ン部生成的111、マスタ類複数的113、SKE O AMセル生成的115およびSKC OAMセル生成的 は、フィルタ21、セッション健抽出部22、マスタ健 検索部23、新セッション駐待機部24、セッション艇 **れる暗号化通信システムの 1 システムを例に、その構成** を示すプロック図である。この図3に示す通信システム では情報サーベ1から送信回システム10を介し受信仰 システム20~ATMセル形式で俯頼を送信する。 ここ [0046] 図3は、本発明の暗号化通信方法が適用さ で送信回システム10の壁管理サーバ11は、セッショ 117により構成される。また、受信側システム20 検索部25およびデコーダ26により構成される。

Channel Identifier)をセッショ 5は、愉報サーバ1から入力したATMセルのヘッダに れたセッション騒を用いてATMセルのペイロードを暗 含まれる宛先情報であるVPi(Virtual Pa thidentifier) /VCI (Virtual は、全VPI/VCI用のセッション雌を配値できるよ うに構成されており、入力したVPI/VCI用のセッ エンコーダ15は、セッション配検緊部13より入力さ 【0047】まず、送信側システム10のエンコーダ1 ション館を検索し、該当するセッション鍵を出力する。 ソ朝後祭第13~送信する。 セッション競技祭第13 身化し、ペイロードを暗身化したATMセルを出力す

入力したATMセルのヘッダに含まれる宛先情報である VPI/VC1を参照し、当受信局で受信資格のあるV PI/VCIであるセルのみを出力し、それ以外の入力 ルのヘッダに含まれる宛先情報であるVP1/VC1を セッション壁検索部25へ送信する。 セッション壁検索 CI用の壁のみを記憶できるように構成されており、入 セルは削除する。 デコーダ26では、入力したATMセ 部25は、当該受信局20で受信資格のあるVPI∕V カしたVPI/VCI用のセッション値を検索し、核当 [0048] 受信倒システム20のフィルタ21では、 するセッション艇を出力する。

【0049】 デコーダ26は、セッション単位独節13 ロードを復身化し、ペイロードを復身化したATMセル より入力されたセッション磁を用いてATMセルのペイ

ン鍵を含む新しいセッション観配送用のSKE OAM 用の韓配送用に用いるマスタ鍵で暗号化し、宛先が当V 【0050】セッション鮭の変更は、送信仰システム1 0の駐管理サーベ11で、セッション鮭の変更を行うV PI/VCIと当VPI/VCI む用いる 粧しい セッツ ョン健を生成し新しいセッション健を当VPI/VCI PI/VCIで、マスタ壁で暗号化した新しいセッショ

Mセルと同じ気先 N P 1 / N C I の糖質 D タイミング通 セッション単校保部13に合まれる当v P 1 /v C 1 用 特団平11-239125 セルを作成し出力する。その後、出力したSKE OA **知用のSKC OAMセルを存成し、込信すると回导に** のセッション値を折しいセッション壁に安贝する。 ø;

たSKE OAMセルの和先VPI/VCIをマスタ酸 PI/VCI用のマスタ艇を検索し、セッション艇抽出 年22へ送信する。セッション駐拉田街22では、マス タ壁検索師23より受信したマスタ艇を用いて、受信し たSKE OAMセルに含まれる暗号化されたセッショ AMセルの受信と簡時に受信したSKC OAMセルの 名光N P I / NCI を存取し、セッション類位数部25 **に送信し、セッション競技烙師25は記憶される当VP** I/NCI用のセッション館や炉しいセッション観に仮 【0051】 政信応宜システム20のセッション管告記 部22では、SKE OAMセルが入力すると、入力し 政務部23に送信する。マスタ競換器部23では、当V ン値を復与し、当VP1/VCI用の折しいセッション 陸を抽出し、新セッション競枠機能24へ送信する。 [0052] 旅セッション館存取用24ではSKC 2

受信局日、憤慨受信局のを持つシステムにおけるセッシ 報送信局で情報受信局A和の趙変更タイミング情報を作 成、送信し、各情報受信局においては、情報受信局Aの みこの髄変型タイミング情報を受信し、情報受信局への [0053] 図4に存斂送信周及び情報受信周A、情報 [0054] 虫ず、情報遊信局で情報受信周A和の変更 用壁物報を作成、送信し、各情報受信局においては、情 報受信向Aのみこの変更用賠償報を受信する。 吹に、情 ョン鮭の変更法を用いる場合のタイムチャートを示す。 セッション館の寮更を完了する。

改、送信し、各債銀受信局においては、情報受信周3の みこの麒旋更タイミング情報を受信し、情報受信BIBの 【0055】次に、情報送信局で情報受信局B粒の仮見 用壁竹類を作成、送信し、各情報受信局においては、情 報送信局で情報受信局日和の壁変更タイミング情報を作 **報受信局日のみこの変更用顧情報を受信する。次に、**

情報送信局で情報受信局の知の観察更タイミング情報を |0056| 最後に、荷魚送信局で荷幣政信局に知の数 作成、送信し、各情報受信局においては、情報受信局に のみこの観賞更タイミング情報を受信し、情報受信局に 更用盤情報を作成、送信し、各情報受信局においては、 情報受信局Cのみこの変更用鏈情報を受信する。次に、 セッション艇の仮見を完了する。 \$

難で暗号化したセッション離を、複数の宛先分配線、送 t。図5に示すパケットでは、情報受信励A、情報受信 **周B、情報受信局C用の変更用鮭情報(各宛先用のマス** [0057]図5に各変更用値情報に各宛先用のマスタ **信する場合の、変叉用盤情報のパケット構成の例を示** のセッション鮭の仮更を完了する。

8

特開平11-239125

【0058】この図5に示す変更用壁情報を用いて、情 を持つシステムにおいて、セッション鮭の変更を行う酢 報送信局、協報受信局A、情報受信局B、情報受信局C のタイムチャートを図6に示す。

情報受信局A~Cでは、予めこの変更用壁情報における 図5に示すA, B, C充の変更用館情報を送信する。各 各元先用の変更用駐惰報の配畝領域を認識しており、そ れぞれ受信した変更用駐惰粮の該当する領域に記載され ている情報を、各情報受信局において予め保存している 各宛先用のマスタ壁で復号化することにより、新しいセ 【0059】図6を参照するに、まず情報送信局より、 シション観を仰る。

[0060] 次に情報送信局で情報受信局A 宛の壁変更 タイミング情報を作成、送信し、各情報受信局において は、情報受信周Aのみこの壁変更タイミング情報を受信 情報受信局Aのセッション壁の変更を完了する。

[0061] 次に、情報送信局で情報受信局B充の鍵変 題のパケット構成の一例を示す。図りに示すパケットで **更タイミング情報を作成、送信し、各情報受信局におい** ては、情報受信局日のみこの雌変更タイミング情報を受 ては、情報受信局Cのみこの鮭変更タイミング情報を受 の情報受信局用として用いる場合の触変更タイミング情 は充先として情報受信局A~情報受信局Cへの同報用の **宛先を用いる。この図7に示す壁変更タイミング情報パ** [0062] 次に、情観送信局で情報受信局に宛の顧変 **哎タイミング情報を作成、送信し、各情報受信局におい** [0063] 図7に1つの鮭変更タイミング情報を複数 間し、ሰ粗受信周Bのセッション鍵の変更を完了する。 信し、情報受信局Cのセッション壁の変更を完了する。

C宛の変更用鮭楠製を作成、送信し、各帽観受信局にお [0064]まず、情報送信局で情報受信局A宛の変更 報受信局Aのみこの変更用鍵情報を受信する。次に、情 **観送信局で情報受信局B宛の変更用鏈情報を作成、送信** し、各情報受信局においては、情報受信局Bのみこの変 **更用雄情報を受信する。次に、情報送信局で情報受信局** る。最後に情報送信局で図りに示す髄変更タイミング情 報を作成、送信し、各情報受信局ではこの鍵変更タイミ 【0065】 次に図9及び図10に示すタイムチャート を参照して、変更用鏈情報に記載のセッション鍵を複数 いては、情報受信局ののみこの変更用鏈情報を受信す 用顱情報を作成、送信し、各情報受信局においては、 ン壁の変更を行う隙のタイムチャートを図8に示す。 ング情報を受信し、セッション壁の変更を完了する。

更タイミング情報を2回ずつ送信し、情報受信局Aにお り情報受信局Aへ、A宛の変更用鍵情報及びA宛の壁変 いて1回目に送信されたA宛の変更用壁情報を情報受信 **同Aで受信できなかった場合のタイムチャートを示して** いる。この場合、1回目に送信されるA宛の変更用鍵情 **報は情報受信局Aにおいて無効とされ、2回目に送信さ** れるA充の変更用鮭情報及びA充の鮭変更タイミング情 **限によりセッション鍵の変更が完了する。**

受信できなかった場合のタイムチャートを示す。この場 し、1回目に送信されたA宛の変更用健情報と2回目に 報を2回ずつ送信し、情報受信局Aにおいて1回目に送 **送信される鍵変更タイミング情報によりセッション鍵の** 借されたA気の壁変更タイミング情報を情報受信局Aで へ、A 宛の変更用麒情報及びA 宛の離変更タイミング情 合、2回目に送信されるA宛の変更用鍵情報は無効と 変更が完了する。

[0066] 図10に、情報送信局より情報受信局A

01

情報送信局、情報受信局 B、情報受信局 b、情報受信局 図11の情報送信局においては、情報サーバより入力さ れ、情報受信局8~情報受信局dへ送信される全ての情 c、情報受信局dを持つシステムの構成の概要を示す。 【0061】図11に本発明を応用した、情報サーバ、 **取の、暗号化処理を行うことになる。** 20

a、情報受信局b、情報受信局c、情報受信局dを持つ 局り宛に送信される情報の暗号化処理を行い、情報送信 [0069] 図13にセッション醚の変更周期を各宛先 毎に変えて行う暗号化通信方法を実現するための情報送 信局内の駐管理サーバの構成の一例を示す。 図13に示 れるセッション健生成部111と、このセッション健生 成部111に順次接続されるマスタ難検索部113、変 **更用雌情報生成部114および健変更タイミング情報生** 【0068】これに対して、応用倒として、図12に倫 システムの構成の概要を示す。図12の情報送信局Aに 周Bにおいては、情報サーバより、情報受信局c及び情 **す壁管理サーバは、第1の壁変更タイミング管理部11** 0 Aと第2の鍵変更タイミング管理部110 Bが接続さ おいては、僧報サーパより、情報受信局a及び情報受信 のため、図12の情報受信局A及び情報受信局Bでは、 図11の情報受信局での処理が分散されることになる。 報サーバ、情報送信局A、情報送信局B、情報受信局 報受信局d宛に送信される情報の暗号化処理を行う。 成部116により構成される。 30 6

ケットを用いて、情報送信局、情報受信局A、情報受信

周B、情報受信周Cを持つシステムにおいて、セッショ

【0070】第1の離変更タイミング管理部110Aで ミング(変更用鮭情報及び鼬変更タイミング情報の送信 間隔)を管理し、例えば10秒毎に第1の壁変更タイミ ノグ管理部110Aで管理する全ての充先のセッション は、各受信局宛信租用の宛先のセッション鍵の変更タイ 難の変更を行う。

数の受信局宛の、番粗等の情報用の宛先のセッション健 [0071]また、第2の観変更管理部110Bでは複

20

方法の有効性について説明する。図9に、情報送信局よ

回だけ同じセッション醚を変更用鏈情報として送信する

情報の送信閒隔)を管理し、例えば5秒毎に第2の髄変 **更管理師110Bで管理する全ての宛先のセッション醚** の変更タイミング(変更用壁筒報及び離変更タイミング

イミング情報は5秒毎に受信されることにより、複数の 受信局宛の、番粗等の情報の宛先用のセッション壁は5 **り毎に変更される。このように目的に合わせてセッショ** 信局用の変更用壁情報及び鍵変更タイミング情報は10 砂毎に受信されることにより、各情報受信局宛情報用の 【0072】これにより、各情報受信局では、各情報受 セッション壁は10秒毎に変更される。また、複数の受 間局宛の、番組等の情報用の変更用鍵情報及び壁変更タ ン雌の変更周期を各宛先毎に変えることができる。

2

同B用の宛先のセッション雌の変更を10秒毎に、情報 受信問A及び情報受信局Bで受信資格を持つ番組1の宛 先用のセッション戯の変更を5秒毎に行うときの情報送 【0073】図14に図13に示す情報送信局内の顧悟 理サーバを持つことにより、情報受信局A及び情報受信 **信局と各情報受信局間のタイムチャートを示す。**

[0074]図14を雰囲するに、番組1用の変更用値 情報及び離変更タイミング情報の送信、A宛の変更用壁 情報及び健変更タイミング情報の送信、B宛の変更用讎 情報及び酸変更タイミング情報の送信をまず行う。

【図面の簡単な説明】

20

【0075】そして約5秒後に番組1用の変更用壁情報 及び盤変更タイミング情報の送信、更に約5秒後に番組 B宛の変更用健情報及び触変更タイミング情報の送信を まず行う。このように情報送倡局内で宛先毎にセッショ 1 用の変更用鍵情報及び観変更タイミング情報の送信、 A宛の変更用鍵情報及び壁変更タイミング情報の送信 ン雌の変更周期を変更することができる。 [0076] 尚、上記の実施形態ではATMに適用した 場合を例にとって説明したが、本発明はこれに限定され ること無く、いかなる形式のパケットを暗号化する暗号 化通信システムにおいても、またいかなる暗号化アルゴ リズムを用いる暗号化通信システムにおいても、またい かなるセッション雌の変更周期をもつ暗号化通信システ ムにおいても適用できる。

[発明の効果] 上述したように本発明の翻求項1および 6 に記載の暗号化通信方法およびシステムによれば、各 変更用鍵情報に各宛先用のマスタ麒で暗号化したセッシ ョン鍵を複数の宛先分配做、送信できるので、各宛先毎 に異なる変更用離情報を作成、送信する場合に比べ、送 **信する変更用鍵情報の個数を減らすことができる。** 【0078】また、鯖水頃2および7に記載の暗号化通 **慣方法およびシステムを用いると、情報送信局より各究** 先毎に変叉用壁筒報を送信し、送信した各変叉用壁筒報 ミング情報を送信する場合に比べ送信する態変更タイミ に記載のセッション難の適用を全宛先用の壁適用タイミ ング情報1つで行うため、各宛先毎に異なる壁適用タイ

⊛

ング桎梏の個数を扱わすことがたきる。

校開平11-239125

貴方法およびシステムを用いると、情報送信局より各債 報受信局へ、変更用壁情報及び壁変更タイミング情報を 複数回送信することから、各情報受信局において、蚊更 め、各情報受信局においてセッション壁の変更を失敗す [0079] 虫た、鯖状煩3および8に配做の暗号化過 再送される変更用館情報及び健変更タイミング情報によ 用壁情報及び壁変更タイミング情報の受信失敗の際に、 りセッション艇の変更を完了せしめることができるた る強率が小さくなる。

a

[0080] 請求項4および9に記載の暗号化通信方法 およびシステムを用いると、情報送信局が複数であるこ とから、1つの情報送信局にかかる処理負荷が軽減され

法およびシステムを用いると、セッション雄の変更周期 [0081] 請求奴5および10に記載の時争化通信力 ション酸の変更周期を、安全性と、変更用値僧仰及び随 変更タイミング情報の送信によるシステムの送信符版へ を宛先毎に変えることができるため、必要に応じてセッ の影響とのトレードオンにより快泊することができる。 【図1】本発明に係る通信システムにおける情報送信局 [図2] 本発明に係る通信システムにおける情報受信局 **り一 実植形態の概略の構成を示すプロック図れめる。**

【図3】本発明に係る通信システムのシステム全体の概 の一段施形態の機略の構成を示すプロック図である。 なの様点をボナブロック図わせる。

[図4] セッション酸変更法を用いる場合の情報送信局 と☆徴受信局との国のタイムチャートである。

[図5] 図1に示す情報送信局から送信される変更用値 位盤の梅成例を示す図である。

30

【図6】図3に示す通信システムで用いられるセッショ / 観変更法における情報送信局と情報受信局間のタイム チャートである。

[図1] 他の顧査型タイミング情報の構成例を示す図む

【図8】他の通信システムで用いられるセッション特徴 **更法における情報送信局と情報受信局間のタイムチャー** 17555. 【図9】1回目に送信された変更用館情報が情報受信周 で正しく受信できなかった場合のタイムチャートであ \$

[図10] 1回目に送信された健変更タイミング情報が 情報受信局に正しく受信できなかった場合のタイムチャ

[図11] 本発明が適用される一般的な通信システムの 収を示すプロック図である

【図12】他の通信システムの構成を示すプロック図で

[図13] 和先年にセッション雌の変更周期を変える方

8

-8

[図]

20 受信側システム 法を実現するための情報送信局内の健管理サーバの構成

を示すブロック図である。

24 新セッション壁待機部 22 セッション健抽出部 21 71114 【図14】 紀先毎にセッション醚の変更周期を変える方 法を適用した情報送信局と情報受信局間のタイムチャー

【図15】 衛虽放送で用いられるスクランブル方法の3 トである。

爪姫時号の概要を示す図である。 10 送信仰システム 1 位根サーバ 【作号の説明】

13 セッション単位保部 1.1 駐管理サーバ

(図)

115 SKE OAMセル生成部 113 マスク健検索部 01

111 セッション健生成部

25 セッション軽検索部

26 73-4

マスタ駐検索部

117 SKC OAMセル生成部

[区]

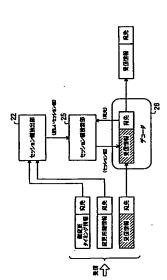
健症更タイミング 情報 情報受信員 人~ C)用 霏仓 を記さが情報 発売 **通回作組 紀先** 民民用組飾館 発先

カンシン加利を取 (カンタンの)

38個數個 和先

(存組政団周人・存取政権国B、 (管観政信風Cへの回絡用名先)

[図2]



情報受信用Aのみ受信 情報受信品人のみ受信 有種交信に8の今交信 新祖安信仰8の少安信 有様受信息ののみ受信 存物の自己Cの少以金 C和観覧戻タイミング情報 B充意変更タイニング情報 A宛戴政民タイミング信仰 A和政党用戰情報 B 投版更用關係組 C和放更用配情報 **全部的和国家** CR歴度更クイミング情報送信 8宛底更用磁情報改造 B内臓疾尿タイミング情報過費 C和数更用解情報送信 ARRE用量情報遊戲 AR製成更タイミング情報送回

(図4)

を開発を表 お記録の 報報 (存成収益的人・存益収益的8.) (存益収益的6.) 存益収益的6.) (存益収益的6.) 水色 心の 甲 公 川田 御 華田 受信氏の用数列用調査論

[図11]

[図2]

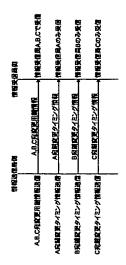
<u>-10</u>

-6-

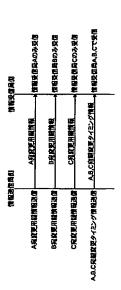
特阻平11-239125

Œ

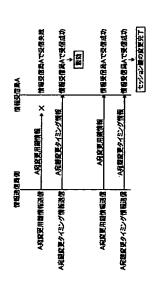
[9 図]



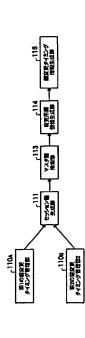
[88]



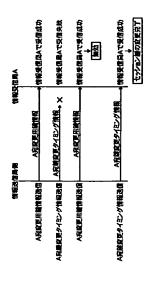
[6図]



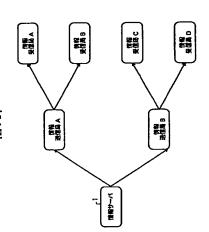
[8813]



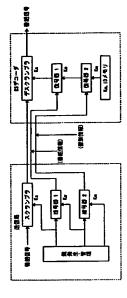
[012]



[图12]



(図15)



-12-

[図14]

10000000000000000000000000000000000000	情報受信局A,Bで受信	情報受信局A,Bで受信	情報受信局Aのみ受信	情報受信局Aのみ受信	情報受信局Bのみ受信	情報受信局Bのみ受信	情報受信局A,Bで受信	情報受信周A.Bで受信)\	情報受信局A.Bで受信	情報受信局A.Bで受信	情報受信局Aのみ受信	情報受信問Vのみ受信	情報受信局Bのみ受信	情報受信局Bのみ受信	
背局側 情報受信局側	番組1の紀先用変更用鍵情報	毎年10%次元 経済更タシッ情報	A和度更用键情報	A和鍵度更列心情報	8宛変更用鍵情報 >	B宛腱変更外沙が情報	番組1の宛先用変更用鍵情報 乗組1のお牛田	銀変更外ジが情報	```	番組1の宛先用変更用鍵情報。	番組1の宛先用 鍵変更外ジグ情報	A和敦田與情報	A宛键变更外沙/情報	B和変更用線情報	B和建度更好沙が情報	
情報送信司風	番組1の宛先用変更用鍵情報送信	番組1の宛先用鍵変更外沙/情報送信	A宛变更用鍵情報送信	A宛鍵変更外沙/情報送信-	8名底更用鍵情報送信	B宛線変更外ジが情報送信・	番組1の宛先用変更用鍵情報送信	断組1の宛先用鍵変更外沙/情報送信	~ <i>(</i>	番組1の宛先用変更用鍵情報送信・	番組1の宛先用鍵変更が沙情報送信	AR胶更用塑情報送信	A充與安更外沿が情報送信	B祝変更用與情報送信	B宛耀斑更外沙/情報送信	

レロントページの類や

(72) 現明者 荒木 克彦 東京都新宿区西新宿三丁目19番2 号 日本電信電話株式会社内 -